National Park Service
U.S. Department of the Interior

Standards of Behavior for the Security of National Park Service Information Resources

May 1st, 2002

NPS Computer User's Acknowledgement of Responsibility

I have read the document entitled "Standards of Behavior for the Security of National Park Service Information Resources". I understand that I am responsible for complying with the rules of behavior set forth in the document. I also understand that I am responsible for any activities that occur through my NPS computer accounts and agree to report any computer security incidents to the appropriate information security representative.

User's full name (Printed clearly) with middle Initial

Signature   Date

Region or Directorate, Park/Center/Office

Submit the completed form with your signature to your supervisor or local information security manager.

Unauthorized use of U S Government computer systems is punishable under Title 18, United States Code, Section 1030

Table of Contents

1. Introduction 1
1.1 What is the Purpose of This Document? 1
1.2 What are Standards of Behavior? 1
1.3 Why are Rules of Behavior Needed? 2
1.4 What are the Penalties for Non- Compliance? 2
2. Standards of Behavior for Computer Users 3
2.1 Official Business 4
2.2 Access 4
2.3 Accountability 5
2.4 Confidentiality 5
2.5 Integrity 6
2.6 Availability 6
2.7 Passwords and User IDs 7
2.8 Hardware 8
2.9 Software 8
2.10 Awareness 9
2.11 Incident Reporting 9
3. Standards of Behavior for Special Circumstances 11
3.1 Privileged Users 12
3.2 Users in Procurement Organizations 13
3.3 Law Enforcement Information Users 13
3.4 Work- at- Home and other Remote Users 14
3.5 Users of Public Access Systems 15
3.6 Users of Personal Information 16
3.7 Managers 17
Appendix A - Security References and Resources 19

1. Introduction

1.1 What is the Purpose of This Document?

The National Park Service is committed to protecting its resources, employees and partners from illegal or damaging actions by individuals, either knowingly or unknowingly. National Park Service information resources, including but not limited to electronically- stored information, computer equipment, software, operating systems, storage media, and network accounts providing electronic mail and web browsing are the property of the federal government and must be protected. The purpose of this document is to explain the statutory requirements for rules of behavior as specified by OMB Circular A- 130, and to establish expectations and accountability for employee behavior while using NPS information resources.

This document does not represent any new policy or law, rather it summarizes existing law and guidance from various NPS and other Federal documents, most specifically the Office of Management and Budget (OMB) Circular No. A- 130, Transmittal No. 3, Appendix III, "Security of Federal Automated Information Resources."

1.2 What are Standards of Behavior?

Standards of Behavior are part of a comprehensive NPS program to provide complete information security.

Effective security is a team effort involving the participation and support of every National Park Service employee and affiliate who deals with information and/or information systems. These guidelines were established to hold users accountable for their actions and responsible for information security. The standards establish ethical and practical rules of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

Standards of behavior tell information users what is expected of them and how to actively protect information. They call on employees to be proactive: by keeping alert to threats and vulnerabilities, staying abreast of security policies and issues, and reporting incidents. Employees are called to act ethically, take initiative, and accept responsibility for safeguarding information resources. It is the responsibility of every computer user to know these standards, and to conduct their activities accordingly

The NPS Information Security Program's Standards of Behavior apply to all employees involved with information resource management (IRM). In addition, these rules apply to all personnel using NPS information resources or providing IRM services (e.g., seasonal employees, contractors, and partners).

1.3 Why are Rules of Behavior Needed?

The primary threats to information security are from the people who access and use the information on a regular basis. The most serious threat to information and systems has always been internal misuse, through user ignorance, incompetence, or malfeasance. With proliferating use of networks, public access systems (including the Internet), and work- at- home programs, users have responsibility for information security more and more in their hands.

Within all computing environments, technical controls alone are not enough to ensure adequate security. Management controls must be used to support and enforce the technical controls.

The Office of Management and Budget has established security requirements for agencies that stress management controls rather than technical controls. A- 130 requires agencies to establish standards of behavior and include them in information security plans. As A- 130 states, standards of behavior help establish a culture of security awareness and responsibility—the best defense against security breaches.

The NPS strategy for implementing standards of behavior incorporates and expands A- 130's requirements. The Program, managed by the NPS Chief Information Office (CIO), focuses on protecting not just automated information systems, but information. Thus, the standards address all forms of information and information resources, manual and automated.

1.4 What are the Penalties for Non- Compliance?

These standards of behavior are founded on the principles described in the NPS published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Standards carry the same responsibility for compliance as the official documents cited above. NPS will enforce the use of penalties against any user who willfully violates any NPS or federal system security (and related), including:

- Official, written reprimands,
- Suspension of system privileges,
- Temporary suspension from duty,
- Removal from current position,
- Termination of employment, and possibly
- Criminal prosecution.

2. Standards of Behavior for Computer Users

Standards, Principles and Rules

The Standards of Behavior are comprised of security principles and rules that establish the expected and acceptable behaviors required to implement those principles. We begin below with a table of principles and follow with individual subsections that discuss each principle in more detail. Each subsection contains the specific 'rules of behavior' related to that principle. Because written guidance cannot cover every contingency, you are asked to go beyond the stated principles and rules, using your best judgment and highest ethical standards to guide your choices and actions.

A summary chart listing the principles of behavior follows:

Principles of Behavior for Computer Users:

1.	Official Business	Employees will use NPS computer systems and information for official business only.
2.	Access	Employees will access and use only information for which they have official authorization.
3.	Accountability	Employees are accountable for their own actions and responsibilities related to information and information resources entrusted to them.
4.	Confidentiality	Employees shall protect confidentially sensitive information from disclosure to unauthorized individuals or groups.
5.	Integrity	Employees must protect the integrity and quality of information.
6.	Availability	Employees must protect the availability of information and systems.
7.	Passwords & User IDs	Employees will protect information security through responsible use of their user IDs and passwords.
9.	Software	Employees will use software in a safe manner that protects software from damage, abuse, and unauthorized use.
10.	Awareness	Employees shall stay informed of security policies, requirements, and issues.
11.	Incident Reporting	Employees will report security violations and vulnerabilities to proper authorities.

2.1 Official Business

Principle: Employees must use NPS computer systems and information for official business only.

Employees must use government information solely to carry out their job responsibilities. Information is invaluable for employees to be effective in their jobs, thus employees are encouraged to use available information to its full potential. At the same time, employees must remember that public service is a public trust—information gained through their NPS employment must be used in accordance with the Constitution, ethical standards, and laws.

Rules:

- When acting in an official capacity, use NPS information and systems strictly to perform official duties, both during work hours and outside of work hours.
- Do not use NPS computers to conduct personal business, play games, or browse the Internet or other on- line services for non- official purposes (note - this needs to be reviewed revised in light of the 'acceptable use policy')

– Do not use government information for private gain, e.g., an employee in a procurement organization must not use knowledge of a pending contract award as a basis for purchasing a vendor's stock.

– Avoid the appearance of using information in a way that is counter to laws and ethical standards.

– Do not use information in any way that

– would adversely affect public confidence in the integrity of the government or the NPS.

– Do not tolerate or collaborate with anyone who uses NPS non- public information or systems for other than official purposes.

– Refer to the following regulatory documents for guidance:

  – 40 CFR 3.104(a), Use of Government Equipment

  – 40 CFR, Chapter 1, Part 3, 3.103, Ethical Standards of Conduct for Employees

  – Privacy Act,

  – Freedom of Information Act,

  <Insert DOI & NPS Directives/Policy references here>

2.2 Access

Principle: Employees shall access and use only information for which they have official authorization.

The security concepts of presumption of denial and least privilege are important to information access. Presumption of denial means only authorized individuals will have access to information. Least privilege means each information user is authorized access only to information needed to carry out job responsibilities. These concepts apply to non- public information and systems, not to public access systems or to information available through a Freedom of Information Act (FOIA) request.

Rules:

- Follow established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards.

– Follow established channels for requesting and disseminating information.

– Do not ask another employee with different or higher access privileges to get information for you.

– Avoid unauthorized "browsing" of information.

– Take measures to limit who can access personal computer files and manual information—only people who need the information should be able to get it.

– Do not give information to other employees or outside individuals who do not have access authority to it.

– Do not store sensitive or confidential information on a system unless access control safeguards (e.g. passwords, locked rooms, protected LAN storage areas) are used

2.3 Accountability

Principle: Employees are accountable for your actions and responsibilities related to information resources entrusted to them.

Accountability can only partially be built into an organization through structure and procedural controls. To a much greater extent, the benefits of accountability depend on the trustworthiness of each employee. It is every employee's responsibility to behave ethically, to develop technical proficiency, and to stay informed about issues and system related to your job

Rules:

- Agree to and participate in accountability controls, such as automated transaction logging and manual logs.
- Behave in an ethically, technically proficient, informed and trustworthy manner when using systems.
- Ensure that no one person has sole access to or control over important information resources.
- Be alert to threats and vulnerabilities such as malicious programs and viruses.
- Acknowledge actions and accept responsibility for correcting errors and rectifying problems.
- Prevent others from using your accounts by using procedures such as the following:
  - Logout or lock the screen when leaving the vicinity of your terminal or PC
  - Set a password on automatic screen savers
  - Password- protect or encrypt sensitive files
- Help remedy security breaches, regardless of who is at fault

2.4 Confidentiality

Principle: Employees must protect confidentially sensitive information from disclosure to unauthorized individuals or groups.

Access to confidentially sensitive information must be restricted to authorized individuals who need it to conduct their jobs. This entails not only refraining from intentional disclosure but also using measures to guard against accidental disclosure. Employees are responsible for both. When an employee changes positions or leaves the NPS, he/she is still obligated to protect the confidentiality of information.

Rules:

- Protect the following kinds of confidentially- sensitive information:
  - *Confidential Business Information (CBI):* trade secrets, proprietary, commercial, financial, and other information afforded protection from disclosure as described in statutes administered by NPS.
  - *Confidential Agency Information (CAI):* information used within the Bureau that, if disclosed, could result in unfair contracting practices or adversely effect NPS personnel or property.
  - *Information protected by the Privacy Act*: personal information about individuals contained in "systems of records," any collection of records on individuals from which information is retrieved by the individuals' names or other personal identifiers.
  - *Enforcement confidential information:* privileged information that, if disclosed, would result in disruption to the legal process or reveal enforcement techniques.
  - *Budgetary information prior to OMB release:* the NPS fiscal budget information prior to its release to Congress by the President.
- Do n't store or transmit confidential information on public- access systems, such as email or the Internet.
- Do not allow unauthorized personnel access to facilities that store or process confidential information.
- Lock up media, such as paper copies, tapes, and disks, containing confidentially sensitive data. Dispose of media according to approved procedures.
- When disposing of media or hardware, ensure that confidential or sensitive data are properly erased. Hard copies of highly sensitive information should be destroyed by pulping or shredding. Highly sensitive information stored on removable media should be entirely erased, or the disks destroyed. When disposing of, or transferring a computer system, follow the Departmental procedure referenced in Appendix A.

2.5 Integrity

Principle: Employees must protect the integrity and quality of information.

Information *integrity* can be corrupted through intentional alteration or accidental damage. Information is of poor *integrity* if Mary's social security number has been altered. Information is of high quality if it is accurate, complete, and up to date. Information *quality* is dependent on its source—it must be correct when created and then must be maintained. For example, information is of poor *quality* if Mary's address is out of date in her personnel file.

Rules:

- Review quality of information as it is collected, generated, and used to make sure it is accurate, complete, and up to date.
- Use protective measures to ensure against accidental loss of information integrity.
- Take appropriate training before using a system to learn how to correctly enter and change data.
- Protect information against viruses and similar malicious code by:
- Using virus detection and correction software
- Avoiding unofficial software, such as shareware and public domain software; and
- Discontinuing use of a system at the first sign of virus infection.
- Prevent unauthorized alteration, damage, unauthorized destruction, or tampering with information.
- Never enter unauthorized, inaccurate, or false information into a system

2.6 Availability

Principle: Employees must protect the availability of information and systems.

Computer systems and media must be protected from environmental factors, such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling. With preparation, employees can minimize the impact of contingencies such as natural disasters, loss of information, and disclosure of information. It is each employee's responsibility to be rehearsed in recovery activities.

Rules:

- Use physical and logical protective measures to prevent loss of availability of information and systems, such as:
  - Perform backups of information on a defined and regular basis,
  - Verify the integrity of the backup media,
  - Practice restoring data from backup media,
  - Store backups in a different building or site from the original data,
  - Maintain an inventory of tapes, diskettes, files and programs,
  - Plan for contingencies.
- Protect systems and media where information is stored:
  - Store media in protective jackets,
  - Keep media away from devices that produce magnetic fields (such as phones, radios and magnets)
  - Keep diskettes away from direct sunlight and store them at acceptable temperatures (50- 110 degrees)
  - Use a filing system to keep track of disks and tapes.
- Take appropriate action to restore availability when information or systems become unavailable due to disaster, damage, or unplanned shutdown:
  - Assess loss or damage, and
  - Restore information from backups
  - Follow contingency plans.
- For important information, ensure that more than one individual knows where to find it and has access rights.

2.7 Passwords and User IDs

Principle: Employees must protect information security through responsible use of user IDs and passwords.

User IDs and passwords are the most widely used security controls for automated information systems. If used properly, they are quite effective in preventing accidental or negligent damage and access. User IDs and passwords are credentials assigned only to one employee. They are used to verify an employees identity within a system and to provide the appropriate level of information access. Audit logs within many NPS systems track activities using these credentials. Employees are ultimately responsible and accountable for any actions taken under their ID. For user IDs and passwords to be effective, employees must follow guidelines for constructing and using them. "Treat your password like a toothbrush: use it every day, change it often, never share it."

Rules:

- Never give a password to another person (including your supervisor or a computer support person).
- Do not ask anyone else for their password.
- If your password becomes known to anyone, **change it immediately**.
- Construct effective passwords:

  What Not to Use

  - Don't use your login name, e.g., smithj, in any form (as- is, reversed, capitalized, doubled, etc.).
  - Don't use your first or last name in any form.
  - Don't use your spouse's or child's name.
  - Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
  - Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
  - Don't use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
  - Don't use a password shorter than six characters.

  What to Use

  - Do use a password with mixed- case alphabetics if system password is case- sensitive.
  - Do use a password with non- alphabetic characters, e.g., digits or punctuation or combine with alphabetic characters, e.g., $robot2!
  - Do use a password that is easy to remember, so you don't have to write it down.
  - Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
- Change passwords frequently—at least every 90 days or immediately when they may have been disclosed.
- Do not write down a password or store it on a computer. (If you must write it down, make sure it is kept on your person or in a sealed envelope in a locked cabinet or safe)
- Enter a password only when no one else is present or ensure they cannot see it.
- Do not attempt to guess at a user ID or password. Guessing on the part of a legitimate user would falsely indicate suspicious activity to the system's audit function.
- Follow login procedures from start to finish without interruption. Never attempt to bypass or automate login procedures that require user ID and password entry.
- Do not build user IDs and passwords into automated procedures, define them by function keys, or program them into applications.
- Be alert to unauthorized attempts to use your user IDs and passwords; immediately report unauthorized access attempts to a security official.

2.8 Hardware

Principle: Employees must protect computer equipment from damage, abuse, and unauthorized use. Each employee has a duty to protect and conserve Federal property, including information processing equipment. Employees have access to many kinds of equipment, from bar code readers to printers, from scanners to plotters, some of it for general use, some of it for use by one individual. Employees must handle equipment carefully by protecting against hazards. Further, employees must prevent problems by performing maintenance regularly.

Rules:

- Protect computer equipment from hazards, such as:
  - Extreme temperatures,
  - Electrical storms,
  - Water and fire,
  - Static electricity,
  - Spills from food and drink,
  - Dropped objects,
  - Dust and dirt, and
  - Combustible materials.
- Keep an inventory of all equipment assigned to you.
- Only use equipment for which you have been granted authorization.
- Do not leave computer equipment in a parked car or in an unsecured location where it might be stolen.
- When equipment requires repair by service personnel, ask to see the service person's identification and keep records of the work performed.
- Follow established procedures when removing equipment from NPS premises. This usually includes getting a property pass.
- Use an uninterruptible power supply (UPS) with your computer to provide protection against electrical power surges, brownouts and outages.

2.9 Software

Principle: Employees must use software in a way that protects user and software from damage or abuse.

Computer users must protect NPS- owned software and protect themselves from malicious software. That is, users are responsible for ensuring that they prevent damage to their operating system software (e.g. Microsoft Windows) and that they prevent damage to their information resources from virus-infected or ill- behaved software.

Rules:

- Use only software authorized by NPS. Do not install non- NPS standard, public domain or shareware software on NPS computers without approval from the appropriate management official.
- Do no use NPS- purchased software on personally- owned or non- NPS computers.
- Do not alter the configuration, including installing software or peripherals, on government computer equipment unless authorized.
- Do not alter software, or allow another person to do so, except as authorized.
- Make backup copies of original sopftware as soon as possible after opening the package. Install from the backup media if possible, retaining the original media in a locked cabinet.
- Scan all new PC software for viruses using approved, current virus scanning software.
- Adhere to software licensing agreements. Copy licensed software only as expressly allowed by the vendor and by NPS organizational policy.
- Maintain an inventory of software licenses and media. Keep media in a locked cabinet or room to prevent theft or unauthorized copying.

2.10 Awareness

Principle: Employees must stay abreast of security policies, requirements, and issues.

Employees must make a conscientious effort to avert security breaches by staying alert to vulnerabilities of NPS information and systems. Employees are in the position to see how security measures are truly used (or not used) and where potential for problems exists. Certain human factors and activities may suggest that fraud or negligence may occur within the organization. Information Security training is mandatory for all NPS employees. Employees are also called on to stay abreast of current security information. It is a quantified fact that knowledgeable employees are an organization's strongest security measure.

Rules:

- Be alert to human factors that may indicate a security risk including: employees with gambling or substance abuse problems, employees who do not take leave, low morale, and poor relationships between management and staff.
- Be alert to clues of abuse:
  - Unauthorized computer products in the office (e.g., games, sports pools, personal business software),
  - Possession of unauthorized equipment, and
  - Unscheduled programs running on a recurring basis.
- Challenge unauthorized personnel in the work area.
- Participate in security training as required.
- Use security training programs and materials.
- Read security information available to employees through E- mail, newsletters, memos, and other sources.
- Follow all security procedures and comply with all policies related to information security.
- If you have questions about the appropriateness of an action or activity, first discuss it with your supervisor or security official.

2.11 Incident Reporting

Principle: Employees must report security violations and vulnerabilities to proper authorities.

Security violations usually consist of every day waste and negligence. Left unchecked, such violations can create a serious problem that requires costly emergency corrective action. It is easy for employees to become complacent if they have never experienced the devastating results of a serious security breach. Nevertheless, it is each employee's responsibility to report any form of security violation, whether it is waste, fraud, abuse, or unethical behavior.

Rules:

- Report security vulnerabilities and violations as quickly as possible to proper authorities so that corrective action can be taken.
- Report vulnerabilities and violations to the appropriate information manager.
- Report emergency incidents to the NPS <Computer Incident Response Team?>
- Take reasonable action immediately upon discovering a violation to prevent additional damage, such as logging out a terminal or locking up property.
- Cooperate willingly with official action plans for dealing with security violations.

[blank page]

3. Standards of Behavior for Special Circumstances

The principles and rules below apply to users in special circumstances. They are meant to provide extra guidance focused on specific situations where users have especially high responsibility for information security. Users addressed below include:

- *Privileged users*, which includes those with special access privileges for development and administration;
- *Users in procurement organizations*, who have access to several kinds of confidentially- sensitive information;
- *Law enforcement users*, who have access to law enforcement confidential information;
- *Work- at- home* employees and other remote users;
- *Users of public access systems*, particularly the Internet;
- *Users of Privacy Act information*; and
- *Managers*, including information system managers and supervisors.

Principles of Behavior for Special Circumstances:

1.	Privileged Users	Privileged users must perform their duties meticulously and reliably in order to preserve information security.
2.	Users in Procurement Organizations	Users in procurement organizations must apply all ethical and legal standards of procurement to their use of information resources.
3.	Law Enforcement Information Users	Users of Law Enforcement information must apply all ethical and legal standards to their use of information resources <any enforcement- specific principles here>.
4.	Work- at- home and Other Remote Users	Work- at- Home and Remote users must establish security standards and apply the rules of behavior at their workplace.
5.	Users of Public Access Systems	Employees shall protect confidentially sensitive information from disclosure to unauthorized individuals or groups.
6.	Users of Personal Information	Users must conduct only legitimate business through public access systems according to authorized procedures.
7.	Managers	Managers must serve as leaders in information security by establishing a culture of awareness, ethical standards, and responsibility.

3.1 Privileged Users

Principle: Privileged users must perform their duties meticulously and reliably in order to preserve information security. Privileged user include:

- System administrators,
- Computer operators,
- System engineers (those with control of the operating system),
- Network administrators,
- Those who have access to change control parameters for equipment and software,
- Data base administrators,
- Those who control user passwords and access levels, and
- Troubleshooters/system maintenance personnel.

Privileged users of information systems must assume a high level of responsibility and initiative for security. With special skills and access rights, privileged users could, through negligence or malicious behavior, wreak havoc on a system. It is critical that they adhere to high ethical standards. It is also critical that they perform their work with meticulous attention to detail.

Privileged users are expected to take initiative in protecting against errors, abuse, and sabotage. Privileged users must make an effort to notice the threats to and vulnerabilities of information systems, calling these to the attention of management and working to develop effective countermeasures. System developers must adhere to sound development practices in the development process. That is, software must be designed and programmed to perform accurately according to user requirements.

Rules: Privileged users will:

- Protect the supervisor or root- level password at the highest level demanded by the sensitivity of the system.
- Use special access privileges only when they are needed to carry out a specific system function.
- Whenever possible, use a non- privileged account.
- Never use special privileges for personal business, gain, or entertainment.
- Use precautionary procedures and technical measures to protect a privileged account from fraudulent use.
- Establish security measures to ensure integrity, confidentiality, and availability of information on systems.
- Watch for unauthorized use of information resources, including the presence of unauthorized software and data.
- Track all security incidents occurring within their area of responsibility.
- Report and investigate all security incidents
- Watch for signs of hacker activity or other attempts at unauthorized access, such as multiple failed login attempts.
- Take appropriate action to reduce damage from security violations, such as disconnecting a PC with a virus from the network or disabling a suspicious user account.
- Alert the appropriate personnel when a system goes down or experiences problems.
- Ensure that systems and data are properly backed up and that the configuration is adequately documented for recovery purposes.
- Assist with recovery activities.

3.2 Users in Procurement Organizations

Principle: Users in procurement organizations must apply all ethical and legal standards of procurement to their use of information resources.

Part and parcel of the job of employees in procurement organizations is daily use of confidentially sensitive information. Specifically, procurement- sensitive information is information about NPS plans and activities related to individual procurements. Employees involved in procurements also use Confidential Business Information (CBI), Confidential Agency Information (CAI), Privacy Act information, and budgetary information extensively.

Disclosure or misuse of such information can cause devastating losses—firms can lose strategic advantage, competition in general can suffer, and NPS can be sued. Employees must adhere to ethical, procedural, and technical standards to safeguard confidentially sensitive information. Employees must not misuse or knowingly disclose procurement- sensitive information.

Laws prohibit employees from using procurement- sensitive information for one's own gain or for another person's gain. For example, when reviewing a proposal, an employee learned of a company's plans to introduce an innovative new product. The employee must not invest in the company on that basis, nor should the employee advise a friend to invest in that company. The employee's duty to protect procurement- sensitive information continues when he/she changes position or leaves NPS. Employees are only justified in disclosing procurement- sensitive information **after** it has been declared in public.

Rules: Users in procurement organizations must:

- Abide by statutes and federal regulations governing procurement- sensitive information, including the following.
  - Disclosure of Proprietary Information, 18 USC 1905
  - Disclosure of Procurement Sensitive Information, 41 USC 423 (b)
  - Freedom of Information Act, 5 USC 552
  - Privacy Act, 5 USC 552(a)
  - Federal Acquisition Regulation, 48 CFR Pt. 3, 14, and 15
- As needed, seek the counsel of an ethics official or security officer.
- Do not use procurement- sensitive information for personal gain.
- Do not endorse products, services, or enterprises related to procurement.
- Do not provide information about a vendor to another vendor.
- Provide all vendors with equivalent information.
- Avoid partiality and the appearance of partiality.
- Do not offer advice to outside parties based on knowledge of procurement- sensitive information.
- Continue to protect procurement- sensitive information from disclosure after changing positions or leaving the NPS.

3.3 Law Enforcement Information Users

Principle: Users of Law Enforcement information must apply all ethical and legal standards to their use of information resources.

<Awaiting input from Law Enforcement review>

Rules: <Awaiting input from Law Enforcement review>

3.4 Work- at- Home and other Remote Users

Principle: Remote users must establish security standards at their workplace sufficient to protect hardware, software, and information.

Remote users of information resources are growing in number. NPS has committed to work- at- home programs. Employees take laptop computers when they travel, which are then used in airplanes and hotel rooms. Engineers and project leaders use computers at NPS field sites. Remote users have a higher level of responsibility for information security for two major reasons: 1) the employee works unobserved; and 2) the work environment falls outside the protection of the NPS facility.

Remote users must establish a standard of self- discipline and initiative that makes productive use of information resources. For example, a work- at- home user may find it especially tempting to use an NPS- owned PC to pay personal bills, send personal email messages, and play games during work hours. Good planning will help prevent waste, errors and abuse.

Remote users must take the initiative to understand issues related to their work environments. This means staying informed of NPS policies concerning work- at- home. It entails reading internal and external literature about security across dial- up lines and use of external systems, such as the Internet.

Rules: Remote users shall:

- Ensure that adequate security provisions are implemented in your remote work environment.
- Have only those resources you really need and have the authority to use.
- Establish a through understanding and agreement with your supervisor as to what your security responsibilities are.
- Use software only according to license agreements- many NPS licensing agreements do not extend to remote use.
- Establish security an appropriate level for the equipment and information in your possession. Ensure that confidential data is secure, and that the dial- in access is secure.
- Use virus protection software on off- site systems and keep it up- to- date.
- Be on the alert for anomalies and vulnerabilities, reporting them to proper officials and seeking advice when necessary.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect passwords from other individuals in your remote workplace. Change passwords more frequently.
- Avoid uploading and downloading sensitive information.

3.5 Users of Public Access Systems

Principle: Users must conduct only legitimate business through public access systems according to authorized procedures.

Information security for public access systems is problematic and requires diligent monitoring. Hackers can get passwords and steal IP addresses. According to the LAN Times, when a user places information on a well- known Internet home page, he or she might as well have put it on a bulletin board at a public library. For some applications, such broad distribution is advantageous. Public access systems provide a wealth of information and resources that NPS employees can use to great advantage in conducting business. NPS encourages their use for legitimate purposes.

Users must remember that publicly available information portrays an image of the NPS to the public. Much of the information placed on NPS public access systems represents NPS policy and positions. Information must reflect high standards of integrity. Users must be careful to avoid the appearance of favoritism to or endorsement of any commercial activity.

Providers of public access systems must establish security measures and gain approvals before making a system available to the public. A risk assessment must be completed so that the appropriate countermeasures can be determined. Security measures must be established to protect the privacy, integrity, and availability of the system and information. Before it is implemented, a publicly available system must be certified and accredited to operate. For existing systems, when a web server or other publicly available server is added, the risk assessment, security plan, and accreditations must be updated.

Integrated email presents special requirements for information security and professional courtesy. It is important to keep distributions lists concise and up to date. Support is provided by central NPS email personnel to ensure that email addresses are unique and properly propagated, and that publicly available groups are maintained.

Rules: Users of Public Access systems should observe the following guidelines:

- When acting in an official capacity, use public access systems for official purposes only.
- Do not browse, chat, or play.
- Do not gather or distribute information for personal gain.
- Place only mission- oriented information on a public access system. Do not place personal or unofficial information on a World- Wide- Web (www) page on the Internet, send it via email, or post it on a newsgroup.
- Do not allow confidential or sensitive information to be sent, received, or access through public access systems. Do not place segments of information on public access systems that could be pieced together to infer confidential or sensitive information.
- Gain approval through established procedures before placing information on a public access system < insert NPS policy/procedure reference here:>
- Ensure that information is accurate and kept up to date.
- Format information to represent a professional image.
- Do not establish hypertext links between NPS web pages and commercial web pages.
- Do not distribute or receive information in violation of copyright laws and intellectual property rights.
- Establish a form of access control, such as a firewall, for all servers connected to publicly available networks.
- Maintain email distribution lists. Include only those who want or need the information. Update lists as frequently as needed, at least annually.
- Process changes in email addresses promptly through the NPS email support team.

3.6 Users of Personal Information

Principle: Users must acquire and use personal information only in ways that respect an individual's privacy.

According to the Information Infrastructure Task Force (IITF) within the Office of Management and Budget (OMB), "information privacy" is an individual's claim to control the terms under which personal information (information identifiable to an individual) is acquired, disclosed, and used. Information privacy is a constitutional right protected by statutes. As technology makes it easier to acquire and edit personal information, those who use it carry increased responsibility to protect it from inappropriate disclosure. While NPS users are accustomed to the concept of protecting personal information that exists within a "system of records", privacy must also be protected whenever personal information is collected, whether the information resides in a system or not. Users of such information must exercise fairness and assume accountability for their actions.

The IITF has developed principles to guide users and providers of personal information, as set forth in the document entitled "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information". The NPS embraces these principles for use by employees. They are summarized below.

Note: The principles do not imply that an NPS employee has the authority to collect personal information at his/her discretion. Collection of personal information is subject to the Privacy Act and NPS policies concerning proper authority to collect information and notify individuals.

Rules: Users of Personal Information will:

- Acquire and use personal information only in ways that respect an individual's privacy.
- Do not improperly alter or destroy personal information.
- Ensure that personal information is accurate, timely, complete, and relevant for the purpose for which it is collected, provided, and used.
- Assess the impact on privacy in deciding whether to acquire or use personal information.
- Acquire and keep only information reasonably expected to support current or planned activities.
- When collecting personal information directly protecting personal information that resides in from an individual provide adequate, relevant, information about:
  - Why the information is being collected;
  - What the information is expected to be used for;
  - What steps will be taken to protect its confidentiality, integrity and quality;
  - The consequences of providing or withholding information; and
  - Any rights of redress.
- Use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.
- Do not use personal information in ways that are incompatible with the individual's understanding of how it will be used.
- Stay informed and inform the public about how information privacy can be maintained.
- Assist individuals in their ability to safeguard their privacy by providing:
  - A means to obtain their personal information;
  - A means to correct their personal information when it lacks sufficient quality to ensure fairness in its use; &
  - The opportunity to remain anonymous when appropriate.

3.7 Managers

Principle: Managers must serve as leaders in information security by establishing a culture of awareness, ethical standards, and responsibility.

Managers can strengthen information security through the culture they promote within their organizations. By following good security practices, managers set an example for employees. Managers must keep their knowledge of security issues and policies current so that they can counsel employees. Ethical practices must be the expected norm. High morale contributes to a good security program. When there is open communication and a good relationship between employees and managers, fewer security violations will occur; those that do are easier to rectify.

Managers must be alert to vulnerabilities and violations within their organizations. They must aware of employees with personal problems, such as substance abuse, financial difficulties, or poor relationships with co- workers. When these problems exist, fraud, waste, and negligence are more likely to occur.

Managers must set up their organizational structures so that everyone is accountable for his/her actions. Otherwise, security breaches will be difficult to detect, correct, and prevent from recurring. The manager is accountable for the activities of the organization as a whole. Two key concepts are important: least privilege and separation of duties. Both of these limit the scope of individual users' functions, making it easier to track their actions.

Even more important is the manager's responsibility to instill an ethical sense of accountability in his/her employees. True accountability relies quite heavily on the responsible nature of employees. Employees are much more likely to admit their errors if they are not in fear of recrimination. In most cases, a manager must focus on resolving a security problem rather than on laying blame or assessing penalties. (Exceptions are cases of blatant negligence or willful abuse.)

Rules: Managers should:

- Emphasize information security as a priority issue with employees. Serve as a leader by setting an example in applying principles.
- Ensure that employees, contractors, partners, etc. have read and are familiar with the Standards of Behavior. that staff are given time to attend information security training, and that they attend appropriate technical training to use computers to perform their functions effectively.
- – Plan and carry out action to reduce damage from security incidents.
- – Track, record, investigate, and resolve all security violations in addition to reporting them to appropriate security officials.
- Take responsibility for restoration of service when a disaster or security violation occurs.
- Be alert for employees with personal problems, such as low morale, substance abuse, financial difficulties, and poor interpersonal relationships, for unauthorized computer products in the work area.
- Establish procedures that promote accountability. and establish separation of duties and access based on the principle of least privilege.
- – When an employee terminates or changes status, take the following actions.
  - – Notify security personnel and system administrators
  - – With friendly terminations, follow an orderly process that guarantees continued availability of the employee's information
  - – Revoke passwords and user IDs.
  - – Retrieve keys to encrypted files.
  - – Find out where information is stored and how to access it.
  - – Obtain documentation and direction on how to perform tasks.
  - – Remind the employee of his/her duty to protect confidential or sensitive information from unauthorized disclosure.
  - – .Terminate the employee's access to information and equipment.
  - – With unfriendly terminations, take quick action to prevent possible sabotage
  - – Physical removal of the employee may be in order.

[blank page]

Appendix A - Security References and Resources

<TBD>